BANDIT Write-up (L0 -L10)

Bandit is a character in a fictional hacking scenario on a website called OverTheWire.org.

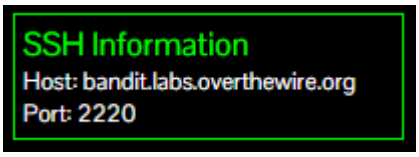
OverTheWire offers a series of wargames designed to teach cybersecurity skills in a safe environment. Bandit is the first wargame in the series, aimed at beginners. It introduces basic *Linux* commands and file manipulation through a series of challenges.

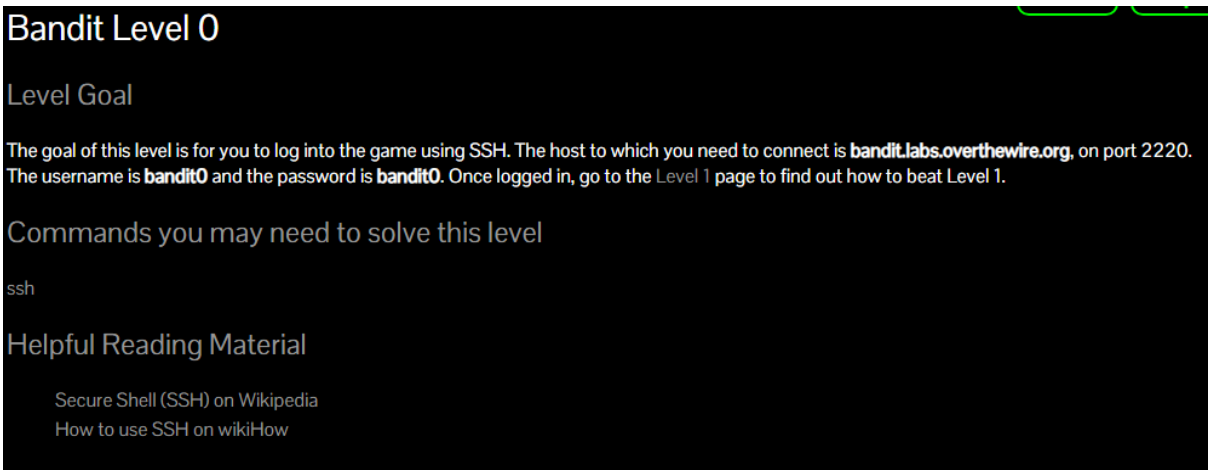
In the Bandit scenario, you play as a new user trying to gain access to higher levels by solving puzzles and cracking passwords. There is no violence or criminal activity involved.

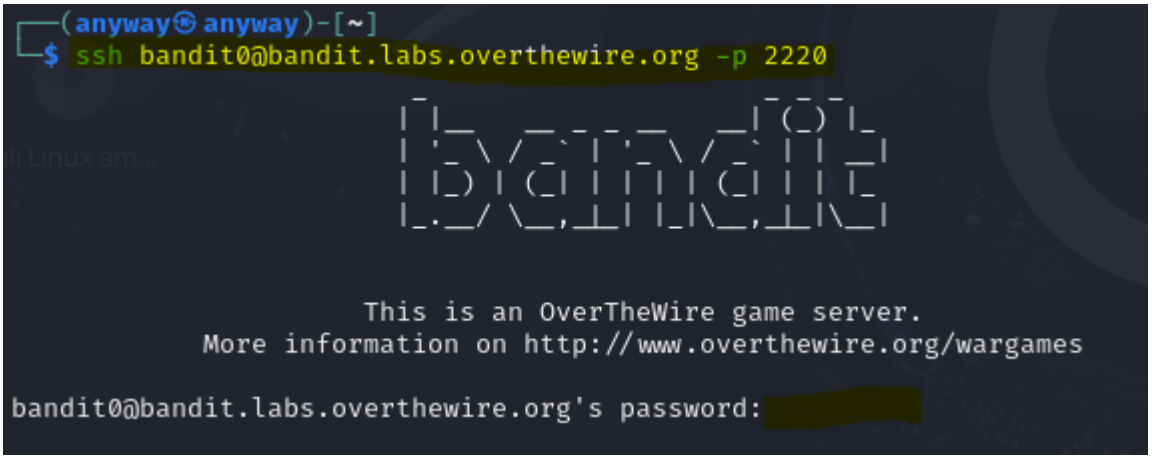
Bandit is the suggested introductory "wargame" within the OverTheWire suite of games. It covers fundamental Linux commands and gradually progresses to advanced techniques as players advance through higher levels. Below are the walkthroughs and methodologies employed to navigate the challenges successfully.

Note for VMs: You may fail to connect to overthewire.org via SSH with a "*broken pipe error*" when the network adapter for the VM is configured to use NAT mode. Adding the setting IPQoS throughput to /etc/ssh/ssh_config should resolve the issue. If this does not solve your issue, the only option then is to change the adapter to Bridged mode.

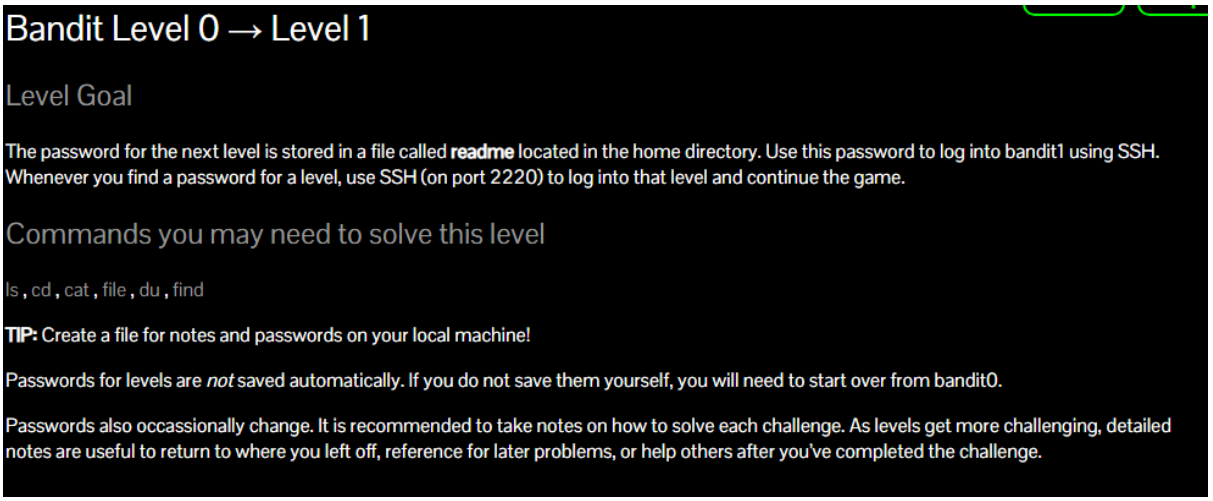
Level 0:

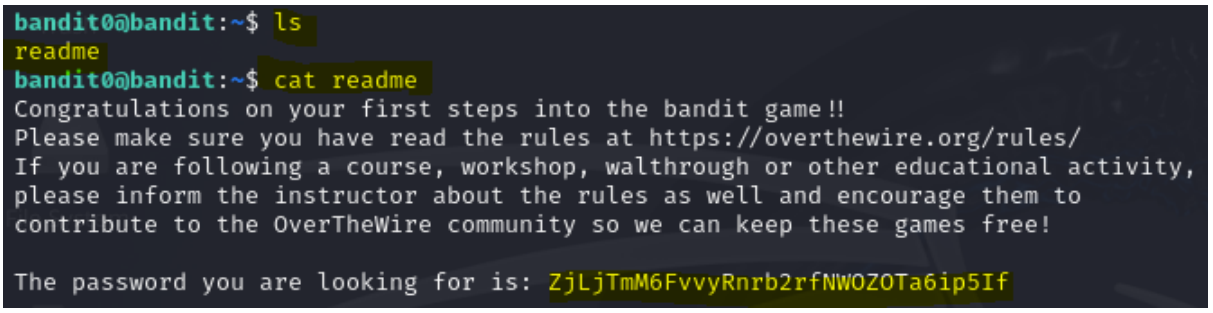






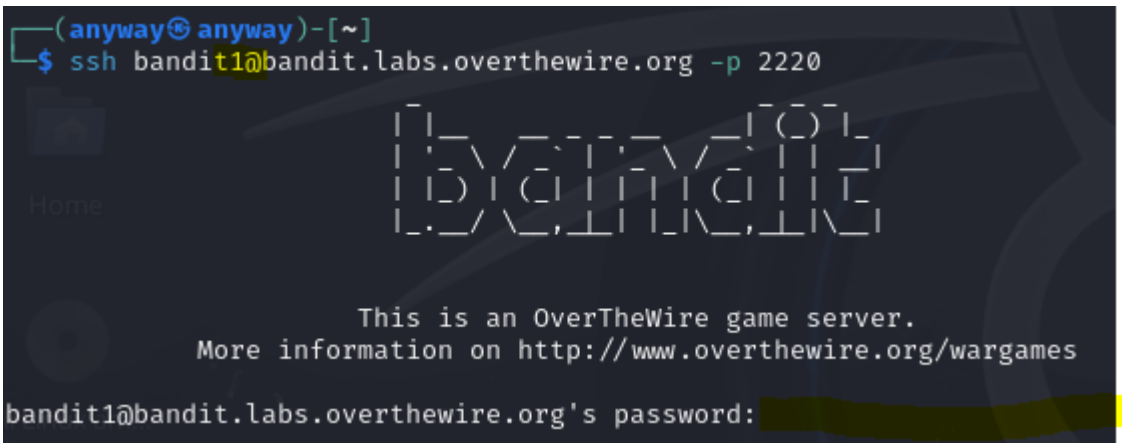
Level 1:



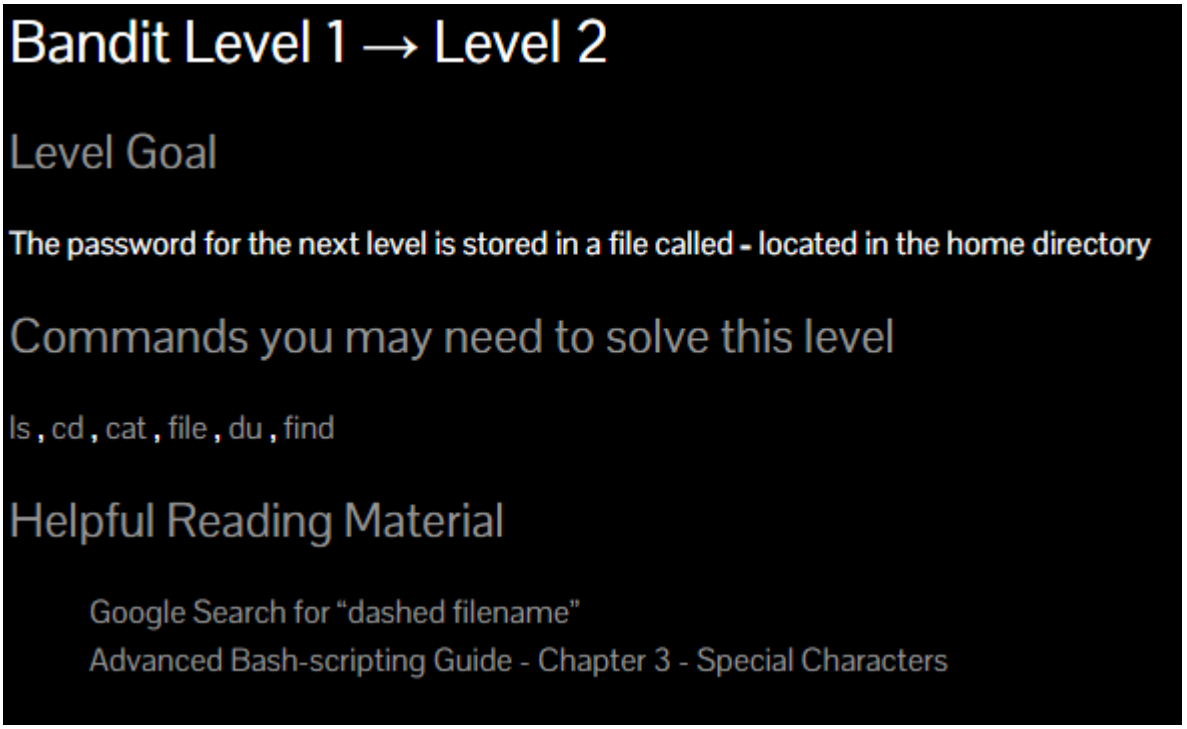


ZjLjTmM6FvvyRnrb2rfNWOZOTa6ip5If

Log in to each level using the same ssh command, and use the username and flag of the previous level to gain access to the next level.



Level 2:



```
bandit1@bandit:~$ ls
-
bandit1@bandit:~$ ls -la
total 24
-rw-r-----  1 bandit2 bandit1   33 Jul 17 15:57 -
drwxr-xr-x  2 root    root    4096 Jul 17 15:57 .
drwxr-xr-x 70 root    root    4096 Jul 17 15:58 ..
-rw-r--r--  1 root    root     220 Mar 31 08:41 .bash_logout
-rw-r--r--  1 root    root    3771 Mar 31 08:41 .bashrc
-rw-r--r--  1 root    root     807 Mar 31 08:41 .profile
bandit1@bandit:~$ cat ./-
263JGJPfgU6LtdEvgfWU1XP5yac29mFx
bandit1@bandit:~$
```

263JGJPfgU6LtdEvgfWU1XP5yac29mFx

Listing shows only (-), so use "*ls -la*" to long list and view hidden files.

- This refers to the current directory.
- This is a wildcard that can match any filename, including hidden files that start with a period (.).

Level 3:

Bandit Level 2 → Level 3

Level Goal

The password for the next level is stored in a file called **spaces in this filename** located in the home directory

Commands you may need to solve this level

ls , cd , cat , file , du , find

Helpful Reading Material

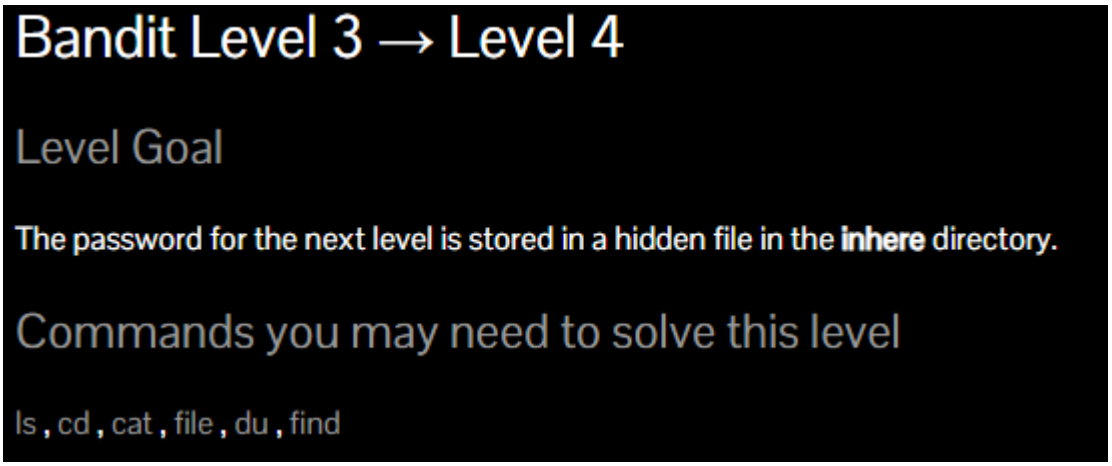
Google Search for "spaces in filename"

```
bandit2@bandit:~$ ls
spaces in this filename
bandit2@bandit:~$ cat ./spaces\ in\ this\ filename
MNk8KNH3Usiio41PRUEoDFPqfxLPlSmx
```

MNk8KNH3Usiio41PRUEoDFPqfxLPlSmx

So, there's a file that contains spaces in its name, we can use (\) this for before spaces to print without error.

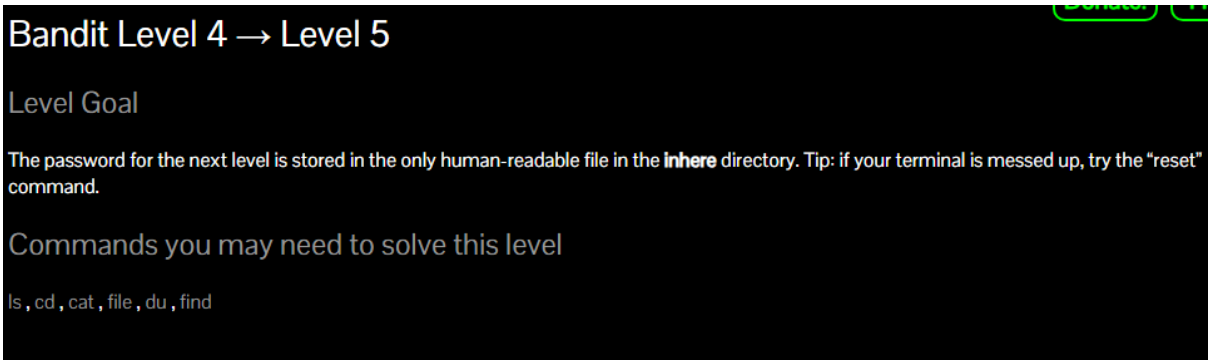
Level 4:

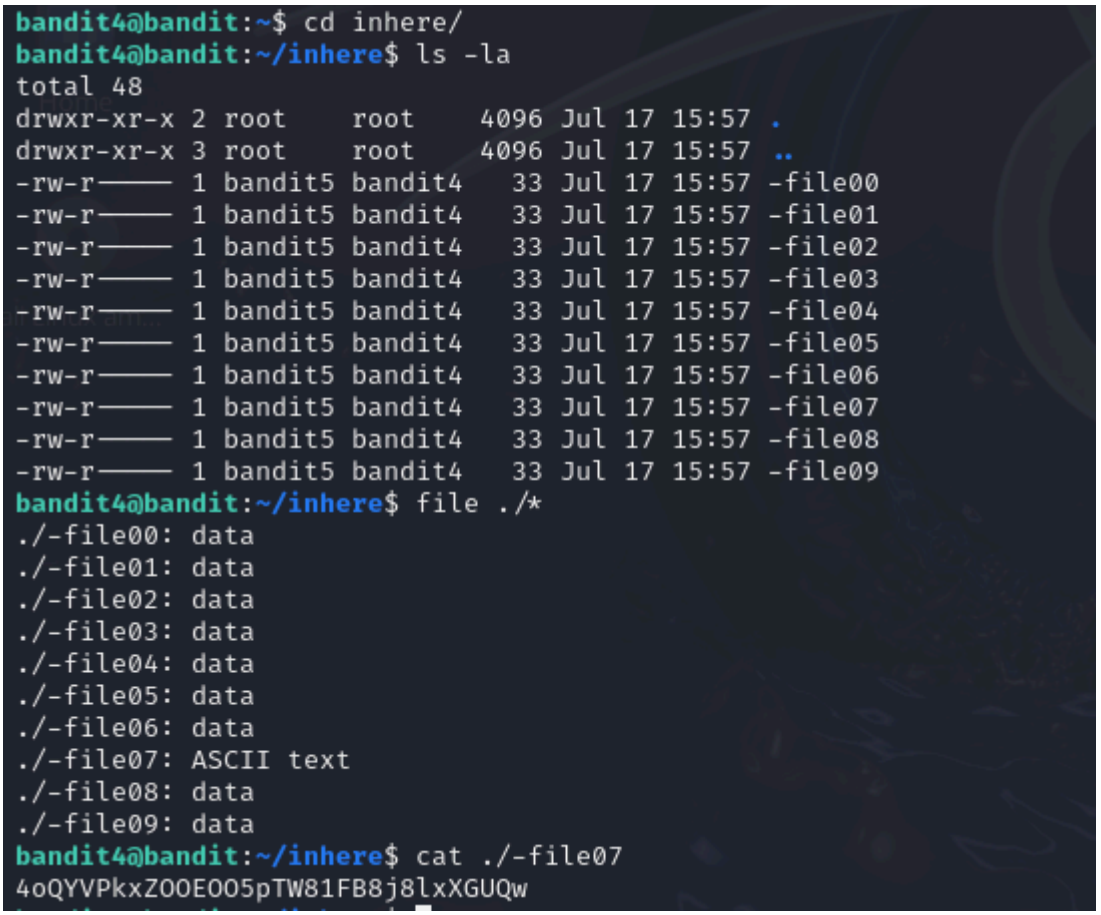



```
bandit3@bandit:~$ ls
inhere
bandit3@bandit:~$ cd inhere/
bandit3@bandit:~/inhere$ ls -la
total 12
drwxr-xr-x 2 root    root    4096 Jul 17 15:57 .
drwxr-xr-x 3 root    root    4096 Jul 17 15:57 ..
-rw-r----- 1 bandit4 bandit3   33 Jul 17 15:57 ...Hiding-From-You
bandit3@bandit:~/inhere$ cat ..
../                 ...Hiding-From-You
bandit3@bandit:~/inhere$ cat ...Hiding-From-You
2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ
```

2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ

Level 5:

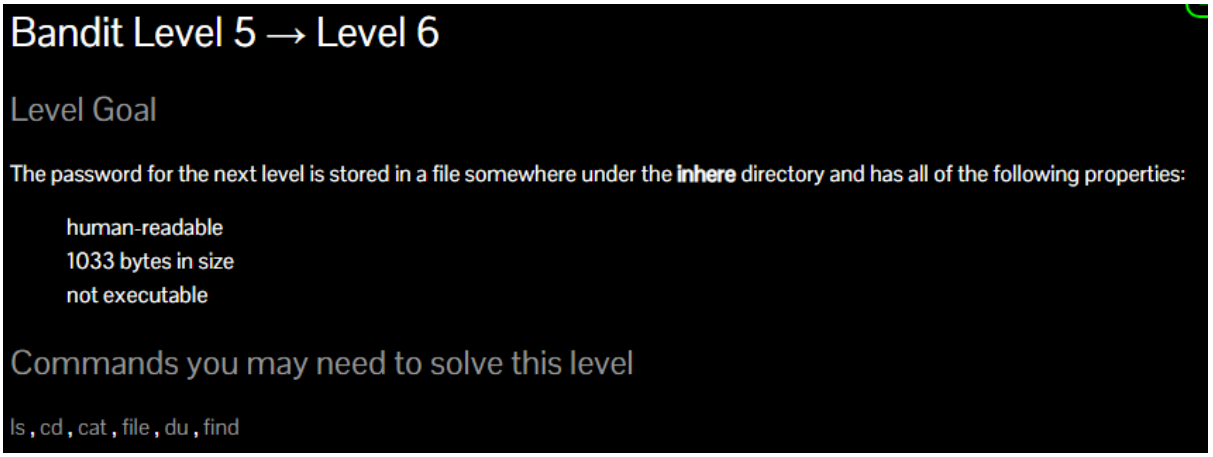




So there were 9 files, with each some written text in different formats, we had to find human-readable text in one of the files. We use ***file ./**** to get the data type in each file. We got ASCII in 7th file, just cat that out:

4oQYVPkxZOOEOO5pTW81FB8j8lxXGUQw

Level 6:



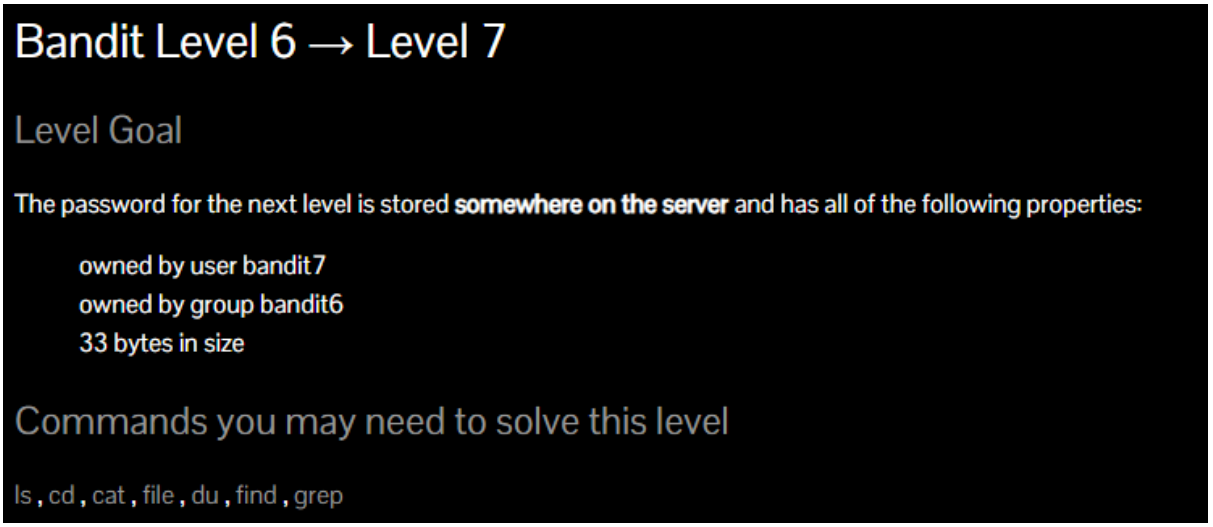

```
bandit5@bandit:~$ ls -la
total 24
drwxr-xr-x  3 root root    4096 Jul 17 15:57 .
drwxr-xr-x 70 root root    4096 Jul 17 15:58 ..
-rw-r--r--  1 root root     220 Mar 31 08:41 .bash_logout
-rw-r--r--  1 root root    3771 Mar 31 08:41 .bashrc
drwxr-x--- 22 root bandit5 4096 Jul 17 15:57 inhere
-rw-r--r--  1 root root     807 Mar 31 08:41 .profile
bandit5@bandit:~$ cd inhere/
bandit5@bandit:~/inhere$ ls -la
total 88
drwxr-x--- 22 root bandit5 4096 Jul 17 15:57 .
drwxr-xr-x  3 root root    4096 Jul 17 15:57 ..
drwxr-x---  2 root bandit5 4096 Jul 17 15:57 maybehere00
drwxr-x---  2 root bandit5 4096 Jul 17 15:57 maybehere01
drwxr-x---  2 root bandit5 4096 Jul 17 15:57 maybehere02
drwxr-x---  2 root bandit5 4096 Jul 17 15:57 maybehere03
drwxr-x---  2 root bandit5 4096 Jul 17 15:57 maybehere04
drwxr-x---  2 root bandit5 4096 Jul 17 15:57 maybehere05
drwxr-x---  2 root bandit5 4096 Jul 17 15:57 maybehere06
drwxr-x---  2 root bandit5 4096 Jul 17 15:57 maybehere07
drwxr-x---  2 root bandit5 4096 Jul 17 15:57 maybehere08
drwxr-x---  2 root bandit5 4096 Jul 17 15:57 maybehere09
drwxr-x---  2 root bandit5 4096 Jul 17 15:57 maybehere10
drwxr-x---  2 root bandit5 4096 Jul 17 15:57 maybehere11
drwxr-x---  2 root bandit5 4096 Jul 17 15:57 maybehere12
drwxr-x---  2 root bandit5 4096 Jul 17 15:57 maybehere13
drwxr-x---  2 root bandit5 4096 Jul 17 15:57 maybehere14
drwxr-x---  2 root bandit5 4096 Jul 17 15:57 maybehere15
drwxr-x---  2 root bandit5 4096 Jul 17 15:57 maybehere16
drwxr-x---  2 root bandit5 4096 Jul 17 15:57 maybehere17
drwxr-x---  2 root bandit5 4096 Jul 17 15:57 maybehere18
drwxr-x---  2 root bandit5 4096 Jul 17 15:57 maybehere19
bandit5@bandit:~/inhere$ find ./ -type f -size 1033c ! -executable 2</dev/null
./maybehere07/.file2
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
HWasnPhtq9AVKe0dmk45nxy20cvUa6EG
```

-type f - filters only regular files.
-size 1033c - size must be 1033 (c - bytes).

! -executable - filter files only executables.
2</dev/null - to hide errors during search.

HWasnPhtq9AVKe0dmk45nxy20cvUa6EG

Level 7:



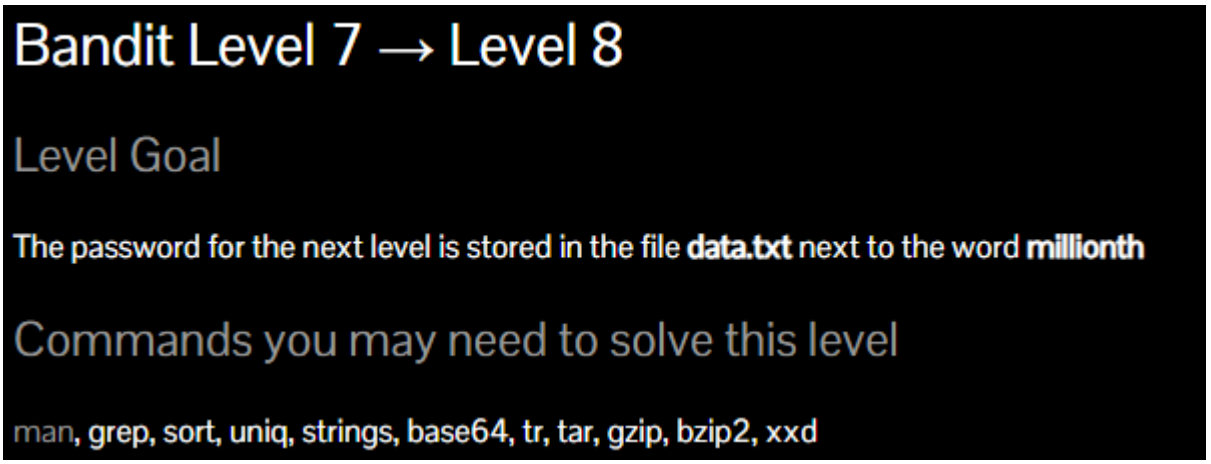

```
bandit6@bandit:~$ find / -type f -size 33c -user bandit7 -group bandit6 2>/dev/null
/var/lib/dpkg/info/bandit7.password
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
morbNTDkSW6jIlUc0ymOdMaLnOlFVAaj
```

The command is the same as previous but with some changes:

Find / - to find files in sub-directories.
-user bandit7 - owned by user bandit7
-group bandit6 - owned by group bandit6

`morbNTDkSW6jIlUc0ymOdMaLnOlFVAaj`

Level 8:




```
bandit7@bandit:~$ ls -la
total 4108
drwxr-xr-x  2 root    root       4096 Jul 17 15:57 .
drwxr-xr-x 70 root    root       4096 Jul 17 15:58 ..
-rw-r--r--  1 root    root        220 Mar 31 08:41 .bash_logout
-rw-r--r--  1 root    root       3771 Mar 31 08:41 .bashrc
-rw-r-----  1 bandit8 bandit7 4184396 Jul 17 15:57 data.txt
-rw-r--r--  1 root    root        807 Mar 31 08:41 .profile
bandit7@bandit:~$ cat data.txt | grep "millionth"
millionth       dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc
```

So we have ***data.txt*** and it contains our flags next to a word *millionth*, so we cat that file, and grep that word, it will print out the whole line.

dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc

Level 9:

Bandit Level 8 → Level 9

Level Goal

The password for the next level is stored in the file **data.txt** and is the only line of text that occurs only once

Commands you may need to solve this level

grep, sort, uniq, strings, base64, tr, tar, gzip, bzip2, xxd

Helpful Reading Material

Piping and Redirection

```
bandit8@bandit:~$ ls -la
total 56
drwxr-xr-x  2 root    root     4096 Jul 17 15:57 .
drwxr-xr-x 70 root    root     4096 Jul 17 15:58 ..
-rw-r--r--  1 root    root      220 Mar 31 08:41 .bash_logout
-rw-r--r--  1 root    root     3771 Mar 31 08:41 .bashrc
-rw-r-----  1 bandit9 bandit8 33033 Jul 17 15:57 data.txt
-rw-r--r--  1 root    root      807 Mar 31 08:41 .profile
bandit8@bandit:~$ sort data.txt | uniq -u
4CKMh1JI91bUIZZPXDqGanal4xvAg0JM
```

So we use ***sort*** to data.txt, which will sort this text file line by line. And ***uniq*** finds a unique line in a text file ***-u*** will remove duplicates.

`4CKMh1JI91bUIZZPXDqGanal4xvAg0JM`

Level 10:

Bandit Level 9 → Level 10

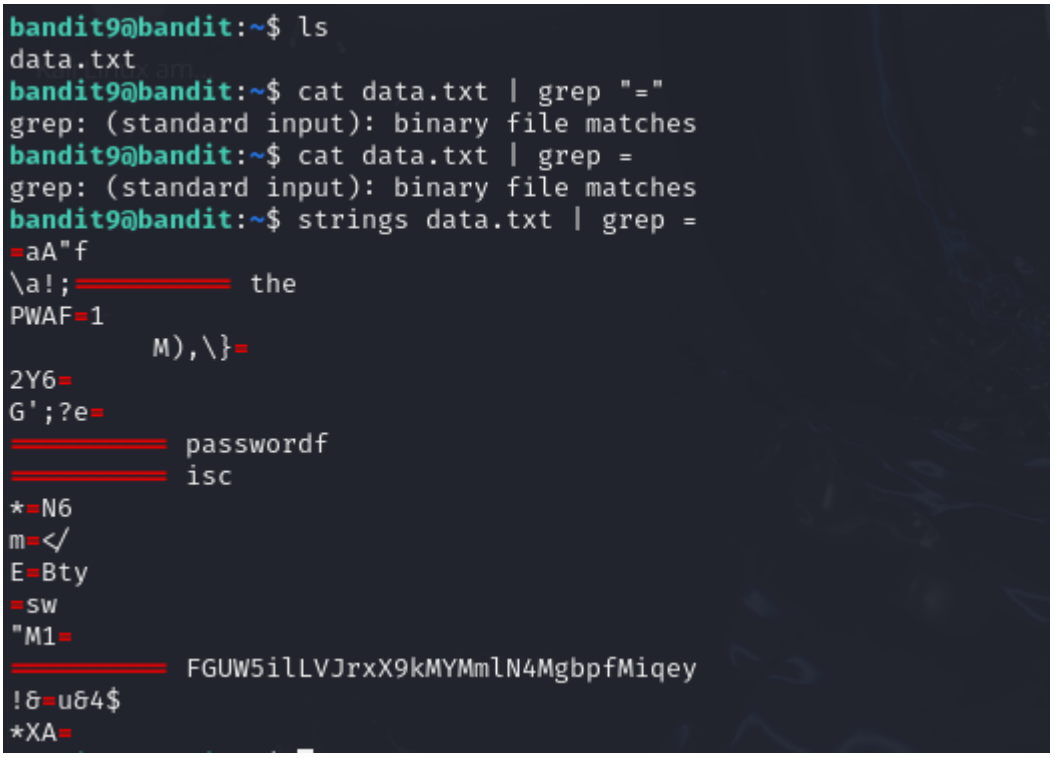
Level Goal

The password for the next level is stored in the file **data.txt** in one of the few human-readable strings, preceded by several '=' characters.

Commands you may need to solve this level

grep, sort, uniq, strings, base64, tr, tar, gzip, bzip2, xxd

So. this command will print only printable strings and grep the = sign:



FGUW5ilLVJrxX9kMYMmlN4MgbpfMiqey

Flags:

1: ZjLjTmM6FvvyRnrb2rfNWOZOTa6ip5If
2: 263JGJPfgU6LtdEvgfWU1XP5yac29mFx
3: MNk8KNH3Usiio41PRUEoDFPqfxLPlSmx
4: 2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ
5: 4oQYVPkxZOOEOO5pTW81FB8j8lxXGUQw
6: HWasnPhtq9AVKe0dmk45nxy20cvUa6EG
7: morbNTDkSW6jIlUc0ymOdMaLnOlFVAaj
8: dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc
9: 4CKMh1JI91bUIZZPXDqGanal4xvAg0JM
10: FGUW5ilLVJrxX9kMYMmlN4MgbpfMiqey